United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 2 p.m. EDT
Wednesday
September 18, 2002

ELECTRONIC GOVERNMENT

Proposal Addresses Critical Challenges

Statement of Linda D. Koontz
Director, Information Management Issues

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to participate in today's hearing on legislation pertaining to e-government. This is an issue of critical importance to the government and its ability to effectively communicate with the public. Recognizing this, both the Congress and current and past administrations have emphasized the importance of e-government[1] and have put forth proposals to address the challenges associated with this issue. Moreover, earlier this year, the Senate passed by unanimous consent S. 803, the E-Government Act of 2002,[2] which was introduced by Senator Lieberman and 14 co-sponsors.[3]

As you are well aware, advances in the use of IT and the Internet are continuing to change the way that federal agencies communicate, use and disseminate information, deliver services, and conduct business. E-government has the potential to help build better relationships between government and the public by facilitating timely and efficient interaction with citizens. The government has not yet fully reached this potential, although substantial progress has been made. Specifically, federal agencies have implemented an array of e-government applications, including using the Internet to collect and disseminate information and forms, buy and pay for goods and services, submit bids and proposals, and apply for licenses, grants, and benefits.

In response to your request, in my remarks today, I will

- briefly describe the background of the federal government's current information resources and technology management framework,
- discuss the challenges facing the federal government in effectively managing information resources and technology,
- discuss the significant legislative provisions intended to address these challenges, and

[1] S. 803 defines e-government as the use of Web-based Internet applications and other information technologies, combined with processes that implement these technologies, to (1) enhance the access to and delivery of government information and services to the public, other agencies, and other government entities or (2) bring about improvements in government operations such as efficiency, effectiveness, and service quality.

[2] S. 803 was introduced in the Senate on May 1, 2001, and a companion bill, H.R. 2458, was introduced in the House of Representatives by Representative Turner on July 11, 2001.

[3] Co-sponsors of S.803 are Senators Bingaman, Burns, Carper, Cleland, Daschle, Dayton, Durbin, Fitzgerald, Johnson, Kerry, Leahy, Levin, McCain, and Stabenow.

- comment on proposed structural changes in OMB to enhance its e-government efforts.

In summary, we strongly support the goal of enhancing the management and promotion of e-government. To accomplish this goal, S. 803 addresses many of the substantive information resource and management challenges facing the federal government today. Initiatives contained in this bill represent important steps in creating a government that is more efficient, effective, and focused on citizens' needs. For example, the bill's provisions would (1) secure the transmission of sensitive information in e-government transactions by promoting the development of electronic signatures, (2) protect individuals' privacy by requiring agencies to conduct privacy impact assessments, and (3) make government information more accessible to the public.

A strength of S. 803's provision to establish an administrator of a new Office of Electronic Government is that it would provide the benefit of a high-level executive position within OMB to focus full time on promoting and implementing e-government. However, a complicating factor is that the federal government's information resources and technology management leadership would be shared between two offices: the proposed new office and OMB's Office of Information and Regulatory Affairs.

Background

The need for strong leadership and an integrated approach to information management has long been recognized as critical. The Paperwork Reduction Act of 1980 established a single policy framework for federal management of information resources and formalized information resources management (IRM) as the approach governing information activities. The Act also gave responsibility to the director of OMB for developing IRM policy and overseeing its implementation. The Clinger-Cohen Act of 1996 amended the Paperwork Reduction Act to give the OMB director significant leadership responsibilities in supporting agencies' actions to improve their IT management practices. These laws created an IRM "umbrella" to govern the management of virtually all federal information activities and to coordinate other laws governing specific information functions such as privacy, security, records management, and information access and dissemination. These other laws include: the Federal Records Act, the Privacy Act of 1974, the Computer Security Act of 1987[4], and the Government Paperwork Elimination Act of 1998.

Under this statutory framework, OMB has important responsibilities for providing direction on managing governmentwide information resources and technology and overseeing agency activities in these areas. Among OMB's responsibilities are

- ensuring agency integration of information resources management plans, program plans, and budgets for acquisition and use of IT and the efficiency and effectiveness of interagency IT initiatives;
- developing, as part of the budget process, a mechanism for analyzing, tracking, and evaluating the risks and results of all major capital investments made by an executive agency for information systems;[5]
- directing and overseeing implementation of policy, principles, standards, and guidelines for disseminating and accessing public information;
- encouraging agency heads to develop and use best practices in IT acquisitions; and
- developing and overseeing implementation of privacy and security policies, principles, standards, and guidelines.

While OMB's director is responsible for these functions, by statute they are delegated to the Office of Information and Regulatory Affairs (OIRA), which was created by the Paperwork Reduction Act. The administrator of OIRA reports to OMB's deputy director for management, described by OMB as the federal chief information officer (CIO). A primary concern we have previously expressed about this structure is that, in addition to their responsibilities for information resources and technology management, the deputy director for management and the OIRA administrator have other significant duties,[6] which necessarily restrict the amount of attention

[4] The Computer Security Act is complemented by the Government Information Security Reform provisions of the fiscal year 2001 Defense Authorization Act.

[5] This responsibility is in addition to OMB's role in assisting the President in reviewing agency budget submissions and compiling the President's budget, as discussed in 31 U.S.C. Chapter 11.

[6] For example, OIRA's other duties include reviewing agency information collection requests under the Paperwork Reduction Act of and reviewing agency rulemaking under presidential executive order.

that they can give to information resources and technology management issues.[7]

Under this statutory framework, agencies, in turn, are accountable for the effective and efficient development, acquisition, and use of information technology in their organizations. For example, the Paperwork Reduction Act of 1995[8] and the Clinger-Cohen Act of 1996 require agency heads, acting through agency CIOs, to

- better link their information technology planning and investment decisions to program missions and goals;
- develop and implement a sound information technology architecture;
- implement and enforce information technology management policies, procedures, standards, and guidelines;
- establish policies and procedures for ensuring that information technology systems provide reliable, consistent, and timely financial or program performance data; and
- implement and enforce applicable policies, procedures, standards, and guidelines on privacy, security, disclosure, and information sharing.

In addition, in June 2001, OMB established the position of associate director for information technology and e-government. This individual is responsible for (1) working to further the administration's goal of using the Internet to create a citizen-centric government; (2) ensuring that the federal government take maximum advantage of technology and best practices to improve quality, effectiveness, and efficiency; and (3) leading the development and implementation of federal IT policy. In addition, the associate director is responsible for (1) overseeing implementation of IT throughout the federal government, (2) working with OMB's deputy director for management to perform a variety of oversight functions statutorily assigned to OMB, and (3) directing the activities of the CIO Council.

The CIO Council is another important organization in the federal information resources and technology management framework that was established by the President in July 1996. Specifically,

[7] U.S. General Accounting Office, *Electronic Government: Challenges Must Be Addressed With Effective Leadership and Management*, GAO-01-959T (Washington, D.C.: July 11, 2001).

[8] The Paperwork Reduction Act of 1995 revised the information resources management responsibilities established under the Paperwork Reduction Act of 1980, as amended in 1986.

Executive Order 13011 established the CIO Council as the principal interagency forum for improving agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources. The Council, chaired by OMB's deputy director for management with a vice chair selected from among its members, is tasked with (1) developing recommendations for overall federal IT management policy, procedures, and standards; (2) sharing experiences, ideas, and promising practices; (3) identifying opportunities, making recommendations for, and sponsoring cooperation in using information resources; (4) assessing and addressing workforce issues; (5) making recommendations and providing advice to appropriate executive agencies and organizations; and (6) seeking the views of various organizations. Because it is essentially an advisory body, the CIO Council must rely on OMB's support to see that its recommendations are implemented through federal information management policies, procedures, and standards. Regarding Council resources, according to its charter, OMB and the General Services Administration are to provide support and assistance, which can be augmented by other Council members as necessary.

Federal Government Faces Significant Challenges in Managing Information Resources and Technology

In executing these broad responsibilities for information resources and technology, the federal government faces significant challenges.[9] To the extent that the billions of dollars in planned IT expenditures can be spent more wisely and the management of such technology improved, federal programs—including e-government initiatives—will be better prepared to meet mission goals and support national priorities. These challenges include:

- *Improving the collection, use, and dissemination of government information.* Agencies are increasingly moving to an operational environment in which electronic—rather than paper—records provide comprehensive documentation of their activities and business processes. This transformation has produced a variety of

[9] U.S. General Accounting Office, *Major Management Challenges and Program Risks: A Governmentwide Perspective*, GAO-01-241 (Washington, D.C.: Jan. 2001) provides an overview of this series. The 2001 *Performance and Accountability Series* also contains separate reports on 21 agencies—covering each cabinet department, most major independent agencies, and the U.S. Postal Service.

issues related to, for example, records management, privacy, and electronic dissemination of government publications.

For example, in July 1999, we reported that the National Archives and Records Administration (NARA) and federal agencies were facing the substantial challenge of preserving electronic records in an era of rapidly changing technology.[10] More recently a 2001 NARA study found that although agencies were creating and maintaining records appropriately, the value of most electronic records had not been assessed nor their disposition determined, as required by statute. Further, records of historic value were not being identified and provided to NARA for preservation, and may be at risk of loss. Our review at four agencies confirmed the results of this study, eliciting a collective estimate that more than 90 percent of mission-critical systems were not inventoried and the electronic records in these systems had not been assessed nor their disposition determined.[11] Improving records management is particularly important in an e-government environment to ensure the appropriate handling of the potentially large number of electronic records generated by transactions between the government and the public.

In addition, the government cannot realize the full potential of the Internet until people are confident that the government will protect their privacy when they visit its Web sites. In September 2000, we reported that most principal Web sites we reviewed (67 of 70) had posted privacy policies that were clearly labeled and easily accessed.[12] However, we also found that of 31 high-impact agencies,[13] most did not post a privacy policy on all Web pages that collected personal information, as required by OMB. In addition, of 101 on-line forms that we reviewed, 44 did not have a privacy policy posted on the Web page. We have made recommendations to strengthen governmentwide privacy guidance and oversight of agency practices that OMB has not yet implemented.

Another important issue involves the use of the Internet and other IT to disseminate government information to the public. Such

[10] U.S. General Accounting Office, *National Archives: Preserving Electronic Records in an Era of Rapidly Changing Technology*, GGD-99-94 (Washington, D.C.: July 19, 1999).

[11] U.S. General Accounting Office, *Information Management: Challenges in Managing and Preserving Electronic Records*, GAO-02-586 (Washington, D.C.: June 17, 2001).

[12] U.S. General Accounting Office, *Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy*, GAO/GGD-00-191 (Washington, D.C.: Sept. 5, 2000).

[13] The National Partnership for Reinventing Government identified 31 agencies as having high impact—that is, they have 90 percent of the federal government's contact with the public.

electronic dissemination offers the opportunity to reduce the costs of dissemination and make government information more usable and accessible—an important aspect of e-government. However, as we reported in March of last year, to move to an environment in which documents are disseminated solely in electronic format, the government would have to ensure that these documents are (1) authentic, (2) permanently maintained, and (3) equally accessible to all individuals.[14] In addition, certain cost issues—including shifting printing costs to libraries and other users—would need to be addressed.

- *Strengthening agency information security.* Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business. However, this widespread connectivity also poses significant risks to our computer systems and, more important, to the critical operations and infrastructure they support, such as telecommunications, public heath, and national defense. Further, the events of September 11, 2001, underscored the need to protect America's cyberspace against potentially disastrous cyber attacks. Finally, as we reported last year, security concerns present one of the toughest challenges to extending the reach of e-government.[15] The rash of hacker attacks, Web page defacing, and credit card information being posted on electronic bulletin boards can make many federal agency officials—as well as the general public—reluctant to conduct sensitive government transactions involving personal or financial data over the Internet.

  Since September 1996, we have reported that poor information security is a widespread federal problem with potentially devastating consequences.[16] Subsequently, in 1997, 1999, and 2001, we designated information security as a governmentwide high-risk area because growing evidence indicated that controls over computerized federal operations were not effective and because the related risks were escalating, in part due to increasing reliance on the Internet. Although agencies have taken steps to redesign and strengthen their information system security programs, our analyses of information security at major federal agencies have shown that

[14] U.S. General Accounting Office, *Information Management: Electronic Dissemination of Government Publications* , GAO-01-428 (Washington, D.C.: Mar. 30, 2001).

[15] GAO-01-959T.

[16] U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

federal systems were not being adequately protected from computer-based threats.[17]

Effective information security is essential to the expansion of e-government. As the government moves toward providing citizens with the capability to conduct the full range of their government business—including sensitive transactions such as benefits applications—on-line, citizens must be assured that these transactions are secure. In addition, unless security features are properly implemented, electronic transactions can be more susceptible to fraud and abuse than traditional paper-based transactions.

A key piece of the solution to the Internet-based security problem will be the development and implementation of the Public Key Infrastructure or PKI technology. A PKI is a system of computers, software and data that relies on certain sophisticated cryptographic techniques to secure on-line messages by attaching so-called "digital signatures" to them. Digital signatures are a special kind of encrypted electronic signature that vouch for senders' identities and establish authenticity of the message to which they are attached. Properly implemented, PKIs can provide the level of security needed to protect the transmission of sensitive transactions, such as those involving personal, financial, and health-related data.

As we reported in February 2001, progress has been made in implementing PKI technology throughout the government.[18] However, because federal agencies are adopting different and potentially incompatible implementations of PKI technology, the development of a Federal Bridge Certification Authority is critical. The federal bridge is being developed to link disparate agency PKI systems and promote interoperability of digital signatures within and outside the federal government. Without a successfully functioning bridge, agencies will need to individually make arrangements to interoperate with other specific agencies in order to share secure information or transactions. This process could prove to be tedious and impractical and, thereby, hamper the expansion of e-government. Consequently, our recommendations for facilitating the adoption of PKI technology in the federal government included one to the Director, OMB, to prepare a

[17] For example, see U.S. General Accounting Office, *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001).

[18] U.S. General Accounting Office, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C., Feb. 26, 2001).

program plan spelling out, among other things, when the federal bridge would be implemented, what resources would be required, and what roles and responsibilities participating agencies would assume. While progress has been made in implementing the bridge, OMB has not yet developed such a plan.

- *Constructing sound enterprise architectures*. Our experience with federal agencies has shown that attempts to modernize IT environments without blueprints—models simplifying the complexities of how agencies operate today, how they want to operate in the future, and how they will get there—often result in unconstrained investment and systems that are duplicative and ineffective. Enterprise architectures offer such blueprints.

  Our February report on the federal government's use of enterprise architectures found that agencies' use of enterprise architectures was a work in progress, with much to be accomplished.[19] In addition, in our testimony before you earlier this year, we noted that the success of the Administration's e-government initiatives hinges in large part on whether they are pursued within the context of enterprise architectures.[20] However, at the time of our testimony, approved architectures for most of these initiatives did not exist. Overcoming this obstacle would be a formidable undertaking even if federal agencies were now successfully using enterprise architectures to manage their respective operational and technological environments, but unfortunately this is not the case. At stake is the ability of federal agencies to not only effectively transform their respective operations and supporting systems environments, and thus elevate their performance, but also to effectively work together in implementing integrated e-government solutions.

- *Fostering mature systems acquisition, development, and operational practices.* High-quality software is essential for agencies' information systems to provide reliable management, financial, and administrative information and to support agencies' many programs. The quality of software is governed largely by the quality of the processes involved in developing or acquiring it and in maintaining it. Using models and methods that define and determine organizations' software process maturity that were developed by

[19] U.S. General Accounting Office, *Information Technology: Enterprise Architecture Use across the Federal Government Can Be Improved*, GAO-02-6 (Washington, D.C.: Feb. 19, 2002).

[20] U.S. General Accounting Office, *Information Technology: OMB Leadership Critical to Making Needed Enterprise Architecture and E-government Progress*, GAO-02-389T (Washington, D.C.: Mar. 21, 2002).

Carnegie Mellon University's Software Engineering Institute, which is recognized for its expertise in software processes, we have evaluated several agencies' software development or acquisition processes. We have found that these agencies' processes do not meet the criteria to be considered at the "repeatable" level of process maturity, which is the second level on the Software Engineering Institute's five-level scale.[21] An organization at the repeatable level of process maturity has the necessary process discipline in place to repeat earlier successes on similar projects. Organizations that do not satisfy the requirements for the repeatable level are by default judged to be at the "initial" level of maturity. This means that their processes are immature, ad hoc, and sometimes even chaotic, with few of the processes defined and success dependent mainly on the heroic efforts of individuals.

In the government's rush to provide greater electronic service delivery, it is essential for agency executives to remember that fundamental principles and practices of good IT planning and management apply equally to effective customer-centric Web-based applications. As we noted in May 2000,[22] some of these fundamentals include

- developing a well-defined project purpose and scope and realistic, measurable expectations;
- understanding and improving business processes before applying technology;
- performing risk assessments and developing appropriate risk mitigation strategies;
- using industry standard technology and solutions, where appropriate;
- adopting and abiding by pertinent data standards;
- thoroughly training and supporting users; and
- reviewing and evaluating performance metrics.

- *Ensuring effective agency IT investment practices.* According to OMB, in fiscal year 2003, federal agencies plan to invest about

[21] For example, see U.S. General Accounting Office, *HUD Information Systems: Immature Software Acquisition Capability Increases Project Risks*, GAO-01-962 (Washington, D.C.: Sept. 14, 2001) and *Customs Service Modernization: Ineffective Software Development Processes Increase Customs System Development Risks*, GAO/AIMD-99-35 (Washington, D.C.: Feb. 11, 1999).

[22] U.S. General Accounting Office, *Electronic Government: Federal Initiatives Are Evolving Rapidly But They Face Significant Challenges*, GAO/T-AIMD/GGD-00-179 (Washington, D.C.: May 22, 2000).

$53 billion to build, operate, and maintain automated systems. If managed effectively, these investments can vastly improve government performance and accountability. If not, however, they can result in wasteful spending and lost opportunities for improving delivery of services to the public. The Clinger-Cohen Act of 1996 requires agency heads to implement a process for maximizing the value and assessing and managing the risks of its IT investments. In support of these requirements, in May 2000 we issued the Information Technology Investment Management maturity framework,[23] which identified critical processes for successful IT investment and organizes these processes into an assessment framework. Using this model, our evaluations of selected agencies found that while some processes have been put in place to help them effectively manage their planned and ongoing IT investments, more work remains.[24]

The importance of effective investment management practices is demonstrated by the government's longstanding problems in developing or acquiring major IT systems. For example, since 1995 we have reported three agency IT modernization efforts as high risk.[25] In some cases, we have seen improvement in the federal government's implementation of major IT investments. For example, earlier this year we reported that the Internal Revenue Service and the U.S. Customs Service had made progress in implementing our past recommendations related to their system modernization projects, although significant work remains.[26]

- *Developing IT human capital strategies.* The challenges facing the government in maintaining a high-quality IT workforce are long-standing and widely recognized. As far back as 1994, our study of leading organizations revealed that strengthening the skills of IT

[23] U.S. General Accounting Office, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, Exposure Draft, GAO/AIMD-10.1.23 (Washington, D.C.: May 2000).

[24] U.S. General Accounting Office, *Information Technology: DLA Needs to Strengthen Its Investment Management Capability*, GAO-02-314 (Washington, D.C.: Mar. 15, 2002); *Information Technology Management: Social Security Administration Practices Can Be Improved*, GAO-01-961 (Washington, D.C.: Aug. 21, 2001); *Information Technology: INS Needs to Strengthen Its Investment Management Capability*, GAO-01-146, Dec. 29, 2000); and *Information Technology Management: Coast Guard Practices Can Be Improved*, GAO-01-190 (Washington, D.C.: Dec. 12, 2000).

[25] U.S. General Accounting Office, *High-Risk Series: An Update*, GAO-01-263 (Washington, D.C.: January 2001); *High-Risk Series: An Update*, GAO/HR-99-1 (Washington, D.C.: January 1999); *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997); and *High Risk Series: An Overview*, GAO/HR-95-1 (Washington, D.C.: February 1995)

[26] U.S. General Accounting Office, *Business Systems Modernization: IRS Needs to Better Balance Management Capacity with Systems Acquisition Workload*, GAO-02-356 (Washington, D.C.: Feb. 28, 2002) and *Customs Service Modernization: Third Expenditure Plan Meets Legislative Conditions, but Cost Estimating Improvements Needed*, GAO-02-908 (Washington, D.C.: Aug. 9, 2002).

professionals is a critical aspect of strategic information management.[27] Moreover, less than a year ago, we reported that, notwithstanding the recent economic slowdown, employers from every sector, including the federal government, are still finding it difficult to meet their needs for highly skilled IT workers.[28]

Without fully developing staff capabilities, agencies stand to miss out on the potential customer service benefits presented by technology and the expansion of e-government. Employees must have the training and tools they need to do their jobs. The process of adopting a new system can be made much less difficult by offering well-designed, user-oriented training sessions that demonstrate not only how the system works, but also how it fits into the larger work picture and “citizen as customer” orientation. A significant challenge for all agencies is providing internal incentives for customer service, reducing employee complaints, and cutting the time that employees spend on non-customer-related activities.

S.803 Provisions Are Important to Addressing Challenges

Recognizing the magnitude of the information management and technology challenges facing the federal government, S. 803 seeks to address many of these challenges through its individual provisions. Next, I would like to comment on significant provisions of the bill concerning improving the collection, use, and dissemination of government information; strengthening information security; meeting IT human capital needs; and establishing the CIO Council in statute.

- *Improving the collection, use, and dissemination of government information.* S. 803 emphasizes that an important goal is using the Internet and other IT to make government information better organized and more accessible to the public. The bill seeks to accomplish this goal first by establishing an interagency committee to make recommendations to OMB on how government information can be better organized, preserved, and made available to public. In turn, OMB is required to issue policies on (1) standards for the organization and categorization of information, (2) the categories of

[27] U.S. General Accounting Office, *Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology*, GAO/AIMD-94-115 (Washington, D.C.: May 1994).

[28] U.S. General Accounting Office, H*uman Capital: Attracting and Retaining a High-Quality Information Technology Workforce*, GAO-02-113T (Washington, D.C.: Oct. 4, 2001).

government information to be classified, and (3) priorities and schedules for the initial agency implementation of these standards.

The proposal for an interagency committee appears to be a reasonable first step to addressing this complex issue; however, we caution that previous attempts to categorize government information have been difficult to implement across federal agencies. For example, the Senate report accompanying the bill concludes that a similar effort to develop the Government Information Locator System (GILS)—required by the Paperwork Reduction Act of 1995—never achieved its goal of facilitating public and agency access to government information. More specifically, a 1997 contractor study done for the General Services Administration reported that while the concept of GILS was sound, its implementation suffered because of many factors including (1) a lack of clarity as to the purpose and benefits of the system, (2) insufficient governmentwide leadership, oversight, and guidance; and (3) inadequate senior agency management attention and allocation of resources.[29] An important role of the interagency committee proposed by the bill would be to consider such "lessons learned" and incorporate them into its recommendations.

S. 803 also recognizes the need to make government information and services available to all citizens, including those without access to the Internet. It requires that when promulgating policies and implementing programs related to providing government information and services over the Internet, agency heads (1) ensure that the availability of government information and services not be diminished for individuals who do not have access to the Internet and (2) pursue alternative modes of delivery. We agree that an important policy consideration governments face is how to provide services and access to segments of the population with limited Internet access and ensure their participation in this new electronic environment. Although a February report by the Department of Commerce found that American's use of the Internet has been impressive—with the percentage of individuals using the Internet more than doubling in about 4 years—in September 2001, about 46 percent of the population was not using the Internet.[30] In addition, more than 60 percent of certain segments of the population were not

[29] William E. Moen and Charles R. McClure, *An Evaluation of the Federal Government's Implementation of the Government Information Locator Service (GILS)*, prepared under contract to the General Services Administration (June 30, 1997).

[30] U.S. Department of Commerce, *A Nation Online: How Americans Are Expanding Their Use of the Internet* (February 2002). This report used data from Commerce's Census Bureau's September 2001 current population survey of approximately 57,000 households.

using the Internet—including Hispanics, individuals without a high school diploma, persons over 50 years old, and those with a family income of less than $25,000. As a result, multiple access methods to government services and processes may be essential to supplement Internet use (e.g., in person, by phone, via fax, using public kiosks).

Regarding privacy, S. 803 also requires agencies to conduct privacy impact assessments before developing or procuring IT, or initiating a new collection of information, that includes any identifier permitting the physical or on-line contacting of a specific individual. Such assessments would include what information is being collected, why it is being collected, and its intended use. Many agencies across government—including the Postal Service and the Internal Revenue Service—are already using privacy impact assessments and have found them useful. This requirement should focus needed agency attention on the privacy implications of collecting personal information and ensure that the use of these assessments continues. In addition, conducting these assessments may help achieve one of the goals of the Privacy Act, to reduce the amount of information that agencies collect, by discouraging agencies from collecting unnecessary personal information and encouraging them to destroy personal information that is no longer necessary.

However, one issue with the privacy impact assessment provision is that S. 803 limits the requirement for these assessments to information systems and collections that include an "identifier permitting the physical or on-line contacting of a specific individual." We note that the Senate committee report accompanying this bill describes such identifiers broadly as including a first and last name; a home or other physical address; an e-mail address; a telephone number; a social security number; a credit card number; or a birth date, birth certificate number, or place of birth. However, without this definition in the bill itself, the requirement could be interpreted more narrowly and may result in these assessments being applied to fewer collections and systems than intended.

The act also requires OMB to develop guidance for privacy notices on agency Web sites used by the public. This is consistent with our September 2000 recommendation that OMB consider, in consultation with appropriate parties such as the CIO Council, how best to help agencies better ensure that individuals are provided clear and adequate notice about how their personal information is treated when they visit federal Web sites.[31]

- *Strengthening agency information security.* S. 803 would repeal the November 29 expiration of the Government Information Security Reform provisions (commonly referred to as "GISRA") in the National Defense Authorization Act for Fiscal Year 2001. We support the continued authorization of GISRA. As we testified in May,[32] based on its first-year implementation, GISRA proved to be a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses. Agencies have noted benefits from GISRA, such as increased management attention to and accountability for information security.

  Mr. Chairman, this provision of S. 803 is also consistent with one purpose of the legislation that you have introduced—H.R. 3844, the *Federal Information Security Management Act of 2002*, which seeks to reauthorize and expand GISRA information security, evaluation and reporting requirements. In our May testimony, we commented on the provisions of H.R. 3844 and supported continued authorization of information security legislation to (1) sustain agency efforts to identify and correct significant weaknesses, (2) reinforce the federal government's commitment to establishing information security as an integral part of its operations, and (3) help ensure that the administration and the Congress continue to receive the information they need to effectively manage and oversee federal information security. In addition, on the basis of our review of first-year GISRA implementation, we noted a number of additional changes proposed by H.R. 3844 that could further strengthen the implementation and oversight of information security in the federal government, such as requiring the development and promulgation of, and agency compliance with, minimum mandatory management controls for security information and information systems.

  S. 803 also includes a provision to further interoperability of electronic signatures for use in securing electronic business transactions with the government. The term "electronic signature" refers to the full range of methods for attaching personal identifiers to electronic documents, including PKI technology. We agree with

[31] GAO/GGD-00-191.

[32] U.S. General Accounting Office, *Information Security: Comments on the Proposed Federal Information Security Management Act of 2002*, GAO-02-677T (Washington, D.C.: May 2, 2002).

the bill's support for digital signatures.[33] We note that while previous versions of the bill authorized funding exclusively for the development of the Federal Bridge Certification Authority, S. 803 as enacted authorizes this funding for the bridge or other activities to promote interoperability of electronic signatures across the government.

- *Meeting IT human capital needs.* S. 803 addresses this critical issue by requiring that, for IT and information resources management, the Office of Personnel Management, in consultation with OMB, the CIO Council, and the General Services Administration, (1) analyze, on an ongoing basis, the government's personnel needs; (2) oversee the development of curricula, training methods, and training priorities that correspond to the projected personnel needs of the government; and (3) assess the training of federal employees in IT disciplines, as necessary. This requirement is consistent with our prior work, which found that leading organizations identify existing IT skills and needed future skills, as well as determine the right skill mix.[34] Accordingly, we suggested that executives should systematically identify IT skill gaps and targets and integrate skill requirements into performance evaluations. In addition, our February 2001 study of public- and private-sector efforts to build effective CIO organizations found that leading organizations develop IT human capital strategies to assess their skill bases and recruit and retain staff that can effectively implement IT to meet their business needs.[35]

- *Establishing the CIO Council in statute.* S. 803 also establishes the existing federal CIO Council in statute. Just as with the Chief Financial Officers' Council, there are important benefits associated with having a strong statutory base for the CIO Council. Legislative foundations transcend presidential administrations, fluctuating policy agendas, and the frequent turnover of senior appointees in the executive branch. Having congressional consensus and support for the Council helps ensure continuity of purpose over time and allows constructive dialogue between the two branches of government on rapidly changing management and IT issue. Moreover, as a prime user of performance and financial information, the Congress can benefit from having the Council statutorily based,

[33] Digital signatures are a special kind of encrypted electronic signature that vouch for senders' identities and establish authenticity of the message to which they are attached.

[34] GAO/AIMD-94-115.

[35] U.S. General Accounting Office, *Executive Guide: Maximizing the Success of Chief Information Officers, Learning from Leading* Organizations, GAO-01-376G (Washington, D.C.: February 2001).

thus providing it with an effective oversight tool in gauging the progress and impact of the Council on advancing effective involvement of agency CIOs in governmentwide IT initiatives.

S.803 Proposes an E-Government Position

To oversee governmentwide implementation of the bill's provisions and other e-government initiatives, S.803 would establish an Office of Electronic Government within OMB headed by an administrator appointed by the President with the advice and consent of the Senate. Under the bill, the administrator would be expected to, among other duties,

- advise OMB's director on the resources required to develop and effectively operate and maintain federal information systems;
- provide overall leadership and direction to the executive branch on e-government by working with authorized officials to establish management policies and requirements for information resources, and by reviewing the performance of each agency in acquiring, using, and managing information resources;
- promote innovative uses of IT by agencies, particularly initiatives involving multiagency collaboration; and
- sponsor ongoing dialogue among federal, state, local, and tribal government leaders on e-government in the executive, legislative, and judicial branches, as well as with leaders in the private and nonprofit sectors, to encourage collaboration and enhance understanding of best practices and innovative approaches in acquiring, using, and managing information resources.

One strength of this approach is that it establishes a high-level executive position within OMB to focus full-time on promoting and implementing e-government. However, a complicating factor is that the federal government's information resources and technology management leadership would be shared between two offices: the proposed Office of Electronic Government and OIRA. The bill addresses this issue by requiring the administrator of the proposed Office of Electronic Government to work with the administrator of OIRA on a variety of information technology and management issues. For example, the administrators of OIRA and the Office of Electronic Government would be responsible for working together on security; privacy; access to, dissemination of, and preservation of government information; the development of enterprise architectures; and capital planning and investment control for IT.

Although a constructive working relationship between the two offices could be established, having the two organizations hold joint responsibility for many information resources and technology management areas may result in a blurring of accountability for addressing critical information management and technology challenges or in significant issues "falling through the cracks." One possible alternative that could be considered is to create a single governmentwide position devoted exclusively to information resources and technology management functions. There are various ways to accomplish this; one approach would be to establish a federal CIO whose responsibilities include both e-government and the other major IT challenges facing the government. In September 2000, we called for the Congress to consider establishing a formal CIO position for the federal government to provide central leadership and support.[36] Consensus has not been reached within the federal community on the structure and authorities of a federal CIO, or even the need for such an office.

Regardless of approach, we believe that strong and effective central management leadership for information resources and technology is needed in the federal government to address the wide range of IT challenges, which include but are not limited to e-government. Increasingly, the challenges that the government faces are multidimensional problems that cut across numerous programs, agencies, and governmental tools. Although the respective departments and agencies should have the primary responsibility and accountability to address their own issues, central leadership has the responsibility to keep all focused on the big picture by identifying the agenda of governmentwide issues needing attention and ensuring that related efforts are complementary rather than duplicative. Further, such leadership can fulfill an essential role by serving as a catalyst and strategist to prompt agencies and other critical players to come to the table and take ownership for addressing the agenda of governmentwide information resources and technology management issues.

[36] U.S. General Accounting Office, *Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges*, GAO/AIMD-00-290 (Washington, D.C.: Sept. 12, 2000).

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the subcommittee may have at this time.

Contact

If you should have any questions about this testimony, please contact me at (202) 512-6240 or via e-mail at koontzl@gao.gov.